العنوان:	خطر الجرائم المعلوماتية
المصدر:	المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية- ICACC - كلية علوم الحاسب والمعلومات - جامعة الإمام محمد بن سعود الإسلامية - السعودية
المؤلف الرئيسي:	كمال، سعاد
مؤلفين آخرين:	بوبكر، الصحبي(م. مشارك)
محكمة:	نعم
التاريخ الميلادي:	2015
مكان انعقاد المؤتمر:	المملكة العربية السعودية. الرياض
رقم المؤتمر:	1
الهيئة المسؤولة:	جامعة الإمام محمد بن سعود الإسلامية. كلية علوم الحاسب والمعلومات
الشهر:	نوفمبر
الصفحات:	206 - 212
رقم MD:	690644
نوع المحتوى:	بحوث المؤتمرات
قواعد المعلومات:	HumanIndex
مواضيع:	الجرائم المعلوماتية
رابط:	http://search.mandumah.com/Record/690644

خطر الجرائم المعلوماتية

سعاد كمال
المدرسة الوطنيّة للمهندسين بتونس
الجمهوريّة التّونسيّة
msouadpop@gmail.com

الصحبي بوبكر
جامعة حائل
المملكة العربيّة السّعوديّة
sahbi.boubaker@gmail.com

الملخص—لمّا كان لكلّ تطوّر ضريبة فانّ تنامي"الجريمة المعلوماتيّة" يعتبر نتيجة عاديّة لتطوّر المجتمع الافتراضي واتّساع رقعته عبر العالم. وبناءاعلى الإحصائيّات الحديثة أضحت "الجريمة المعلوماتيّة" خطرا حقيقيّا يهدّد أمن الفرد و المجتمع. بل أصبح هذا النوع من الجرائم من بين أخطر الجرائم التّي تقترف في الدول المتقدّمة كأوروبا و أمريكا. لذا فانّ معرفة ماهيّة الجرائم المعلوماتيّة و خصائصها و طبيعتها يتخذ أهميّة بالغة للتّعامل مع هذه الظّاهرة و مخاطرها الاقتصاديّة و الأمنيّة و الاجتماعيّة و الثقافيّة. وماهدفنا في بحثنا المتواضع هذا إلاّ تسليط الضّوء على هذاالنّوع من الجرائم قصد التوعية بخطورته وبيان مايجب فعله للتصدّي له لمنعه أو لتقليص تأثيره.

الكلمات المفتاحيّة: الجرائم المعلوماتية، الإنترنت، خصائص الجرائم المعلوماتيّة و صفات مرتكبيها، تصنيف الجرائم الالكترونيّة، طرق مكافحة الجرائم الالكترونيّة

١. المقدمة

نتيجة ظهور الشبكة العالمية بكل ما حملته من تقدم وخدمات، وتغيير نمط حياة المجتمعات و مع الانتشار الواسع لاستخدامات الإنترنت باعتبارها وسيلة اتصالات عالمية تعتمد على البرامج المعلوماتية الحديثة في ضبط مختلف البيانات والمعطيات المعلوماتية الدقيقة، تحوّل العالم إلى قرية صغيرة (انظر الشّكل رقم (١)) من حيث الأحداث و الوقائع التي يمكن متابعتها في أيّ زمان ومكان، بل لحظة حصول الحدث ذاته.



شكل رقم (١): العالم وحدة واحدة لا تعرف الحواجز الجغرافيّة

لكن للأسف تمّ اساءة استخدام معالم هذه الثّورة المعلوماتيّة لتصبح عالما من عوالم الجريمة التي أضرّت بالناس ومصالح الدول بأسرها. يقول الدكتور محمد صالح العادلي أستاذ القانون الجنائي بكليّة الحقوق بمسقط وجامعة الأزهر بمصر، محامي بالمحكمة العليا الدستورية بمصرا1]" [
الجريمة الالكترونية هي: الابن غير الشّرعيالذي جاء نتيجة للتّزاوج بين ثورة تكنولوجيا المعلومات مع العولمة، أو هي الماردالذي خرج من القمقم ولا تستطيع العولمة أن تصرفه بعد أن أحضرته الممارسة السيّئة لثورة تكنولوجيا المعلومات".

في بحثنا اليوم سنحاول التّطرق إلى تعريف هذه الجرائم وأنواعها وخصائصها لنصل في الأخير إلى إجابة لإشكاليّة فرضت نفسها مؤخّرا ألا وهي: ما هو واقع الجرائم الالكترونيّة اليوم وما هي سبل الحدّ من هذه الآفة الخطيرة والسريعة. ويجدر الإشارة هنا أنّه اذا قلنا الجريمة المعلوماتيّة أو الجريمة الالكترونيّة أو جرائم الإنترنت فنحن نقصد بذلك نفس الشيئ و إن تعدّدت المسميّات.

٢. تعريف الجرائم المعلوماتيّة

أدّت الحداثة التي تتميّز بها الجريمة المعلوماتيّة و اختلاف النّظم القانونيّة بين الدّول، الى عدم الاتّفاق على مصطلح موّحد للدلالة عليها. فبعد أن كان الاعتداء على الاموال يتمّ بواسطة السرقة التقليدية أو النصب، و كانت الثقة في المحررات الورقية يعتدى عليها بواسطة التزوير، أصبحت هذه الأموال يعتدي عليها عن طريق اختراق الشبكات المعلوماتيّة واجراء التحويلات الالكترونيّة من اقصى مشارق الأرض الى مغاربها في لحظات معدودة، كما اصبحت تلك الحقوق الثابتة في الأوعية الورقيّة يتمّ الاعتداء عليها في أوعيتها الالكترونيّة المستحدثة عن طريق اختراق الشّبكات والانظمة المعلوماتيّة دون الحاجة الى المساس بايّ وثائق أو محرّرات ورقيّة.

وبعد ان كانت الحياة الخاصة للإنسان تواجه الاعتداء باستراق السمع او الصورة الفوتوغرافية، اصبحت هذه الخصوصية تنتهك بواسطة اختراق (انظر الشّكل رقم (٢)) البريد الالكتروني والحواسب الشخصية ، و قواعد البيانات الخاصّة بالتأمين الصّحي والمستشفيات ومؤسّسات الائتمان والتأمين الاجتماعي2].]



شكل رقم (٢): الجريمة المعلوماتيّة

عرفّت الجريمة بصفة عامّة على أنّها كلّ فعل غير مشروع صادر عن ارادة آثمة يقرّر له القانون عقوبة أو تدبيراحترازيّا [3].

أمّا شرعا فعرفّت الجريمة بأنّها اتيان فعل محرّم معاقب على فعله أوترك فعل محرّم الترك معاقب على تركه، أو هي فعل أو ترك نصّت الشريعة على تحريمه و العقاب عليه 4].] وأمّا الجريمة المعلوماتيّة فقد تعدّدت التعاريف بشأنها:

أ) التعريف الأوّل:

يعتمد هذا التعريف على وسيلة ارتكاب الجريمة، فطالما أنّ وسيلة ارتكاب الجريمة هو الحاسوب أو احدى وسائل التقنية الحديثة المرتبطة به فتعتبرمن جرائم الإنترنت3].] إذا فالجريمة الالكترونيّة هي نشاط اجرامي يستخدم فيه الحاسب و الشبكات العالميّة بطريقة مباشرة أو غير مباشرة امّا كوسيلة لتنفيذ الفعل الاجرامي المستهدف و امّا كوسيلة مساعدة لارتكاب جريمة مثل النصب و الاحتيال و غسل الأموال و تشويه السمعة و السبّ.

ب) التعريف الثاني:

يعتمد هذا التعريف على أساس توافر المعرفة بتقنية المعلومات. فجرائم الإنترنت هي ذلك النوع من الجرائم التي تتطلّب الماما خاصّا بتقنيات الحاسب الآلي و نظم المعلومات لارتكابها أو التحقيق فيها و مقاضاة فاعليها 3].]

ت) التعريف الثالث:

يعتمد هذا التعريف على أساس موضوع الجريمة، فتصبح الجريمة المعلوماتيّة كلّ تصرّف غير مشروع من أجل القيام بعمليّات الكترونيّة تمّس بأمن المعلوماتيّة و المواضيع التي تعالجها 3].]

ث) التعريف الرابع:

يعتمد هذا التعريف على دمج التعاريف السابقة، فتصبح الجريمة المعلوماتيّة هي الجريمة التي يستخدم فيها الحاسب الآلّي كوسيلة أو أداة لارتكابها أو يمثّل اغراء بذلك، أو جريمة يكون الحاسب نفسه ضحيّتها 3].]

٣. خصائص الجريمة المعلوماتيّة

للجريمة المعلوماتيّة خصائص وسمات تميّزها عن غيرها من الجرائم التقليديّة. وسوف نبيّن هذه الخصائص على النحو الآتي:

أ) جريمة عابرة للحدود:

الجريمة المعلوماتيّة جريمة "عابرة للقارّات" بمعنى أنّها لاتعترف بالحدود الجغرافيّة فهي تتّم عبر شبكات تخترق الزمان و المكان دون ان تخضع لحرس الحدود. إذ بالامكان ارتكابها عن طريق حاسوب موجود في دولة معيّنة بينما يتحقّق الفعل الإجرامي في دولة أخرى أوحتّى في دول عدّة

مثل جرائم نشر المواد ذات الخطر الديني أو الأخلاقي أو الأمني.

ب) جريمة تعتمد على الذكاء في ارتكابها:

مرتكب الجريمة المعلوماتية يتميز بأن لديه معرفة و خبرة في مجال أنظمة الحاسب الآلي و الشبكات بينما مرتكب الجريمة التقليدية كالسرقة و الرشوة و التهريب لا يشترط أن يكون على قدر من التحصيل العلمي و الثقافة.

ت) جريمة ناعمة:

الجريمة المعلوماتية جريمة "هادئة" بمعنى أنها لا تحتاج الى العنف أو أي أدنى مجهود عضلي كجرائم الاغتصاب و القتل، وركنها المادي قد لا يتجاوز مجرد لمسات بسيطة للوحة مفاتيح الحاسب (KeyBoard).

ث) جريمة صعبة الاكتشاف:

معظم الجرائم المعلوماتية تم اكتشافها بالصدفة و بعد وقت طويل من ارتكابها. بل ان عدد الجرائم الالكترونية التي لم تكتشف أكثر بكثير من التي تم كشف الستار عنها. ذلك لأن المجني عليهم غالبا (المؤسسات المالية و الادخارية و الاستثمارية) لا يقومون بالتبليغ عن الجريمة خوفا من التشهير و فقدان ثقة المساهمين و العملاء.

ج) جريمة صعبة الإثبات:

الجريمة المعلوماتية جريمة "صعبة الإثبات" سواء من حيث وسيلة الإثبات أو القائم به. فمن حيث الوسيلة فهي لا تترك أثرا فما هي إلا أرقام تدور في السجلات مما يجعل أمر طمس الدليل من قبل الفاعل و محوه كليا باستعمال البرامج المخصصة لذلك أمرا في غاية السهولة. زد على ذلك نقص الخبرة الفنية و التقنية لدى الأجهزة الأمنية و القضائية لاسيما العربية منها.

٤. خصائص الجناة في الجريمة المعلوماتية

يمكن تصنيف مرتكبي الجريمة المعلوماتية حسب خطورة العمل الإجرامي.

أ) أصناف مجرمي الإنترنت:

- القراصنة الهواة (Hackers): صغار اصطلح على تسميتهم بالعابثين وهم فئة من صغار السن مولعين بالحاسب الآلي، وهي الفئة الأقل خطورة إذ ترتكب المخالفات غالبا عن غير قصد، عن غير إرادة تامة بالأضرار.
- القراصنة المحترفون (Crackers): تتميز هذه الفئة بالخبرة و المهارة العالية في مجال الحاسب الآلي.
- المتطرفون الفكريون: يقومون بترويج موادهم الفكرية المتطرفة عبر الإنترنت.
- المتجسسون: تعمل هذه الفئة على الحصول على معلومات تخص الأعداء.
- مخترقو الأنظمة: تقوم هذه الفئة بالتعرف على مواطن الضعف في الأنظمة المعلوماتية.

ب) صفات مجرمي الإنترنت:

الجاني في جرائم الحاسب الآلي يتمتع بقدر كبير من الذكاء علاوة على أنه إنسان اجتماعي بطبيعته. وتمتعه بدرجة عالية من الذكاء المعلوماتي، تجعل من الصعب تصنيفه بحسب التصنيف الإجرامي المعتاد. لذا ينظر في تحديد أنواع الجناة في الجرائم الالكترونية إلى الهدف من ارتكاب المجرم لجريمته.

الجاني في الجرائم الالكترونية هو إنسان متوافق مع المجتمع حيث أن ذكاءه يساعده على عملية التكيف مع هذا المجتمع، ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو لمجرد إظهار تفوقه على جهاز الحاسب.

ت) أهداف مجرمي الإنترنت:

تعددت أهداف مجرمي الإنترنت وتباينت. فمثلا مجموعة "أنونيموس" (انظر الشكل رقم (٣)) التي قامت باختراق عدة مواقع الكترونية كالموقع الرسمي لراشد الغنوشي تقول بأن هدفها هو مقاومة الرقابة وحماية حريات التونسيين.



شكل رقم (٣): مجموعة أنونيموس الناشطة عبر الإنترنت

يمكن حصر أهداف مجرمي الإنترنت في:

- تحقيق الكسب المادي
- الرغبة في التعلم

- اثبات الذّات
- المزاح والتّسلية
- الفضول والمغامرة
- التشفّي والانتقام

٥. صور الجريمة المعلوماتيّة

للجرائم المعلوماتيّة صور متعدّدة (انظر الشّكل رقم (٤)) يمكن أن نذكر منها أكثرها انتشارا:

أ) جرائم الاختراق:

الإختراق بشكل عام هوالقدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحمايةالخاص بالهدف يستطيع المخترق من خلالها دخول أجهزةالآخرين عنوة ودون رغبة منهم وحتى دون علم منهم. ويعتبرالهجوم على المواقع واختراقها على شبكة الإنترنت من الجرائم الشّائعة في العالم وتشمل جرائم الاختراق تدمير المواقع، اختراق المواقع الرسميّة و الشخصيّة، اختراق الأجهزة الشخصيّة، اختراق البريد الإلكتروني و الإستيلاء على اشتراكات المستخدمين و أرقامهم السريّة و ارسال الفيروسات قصد العبث و التدمير. تتمّ عمليّة الإختراق عادّة عبر برمجيّات خاصّة.

ب) جرائم القرصنة:

جرائم القرصنة تعني الإستخدام أو النسخ الغير مشروع لنظم التشغيل أو لبرامج الحاسب الآلي المختلفة والإستفادة منها شخصيّا أو تجاريّا. ومع تطوّر تكنولوجيا المعلومات، تزايدت المواقع التي تعرض برامج مقرصنة مجّانا أو مقابل مبلغ رمزي وهذا من شأنه أن يسلب حقّ المنتج الاصلي ويعرضه لخسائر كبيرة .

ت) السّرقة و الاحتيال:

لمّا أصبحت معظم المعاملات التجاريّة من بيع و شراء تتمّ من خلال شبكة الإنترنت، تفاقمت عمليّات السرقة و الغشّ فتزايد عدد السلع الوهميّة المعروضة كما تزايد عدد بطاقات الإئتمان المسروقة. و تتصدّر المزادات على الإنترنت قائمة السّرقات و المخادعات.

ث) القمار وغسيل الأموال:

في الماضي، كان لعب القمار يستلزم وجود اللاعبين معا على طاولة واحدة، أمّا الآن، في الكازينوهات الافتراضيّة، يستطيع الشخص أن يمارس القمار دون أن يغادر منزله. كذلك فانّ غسيل الأموال الذي يعني أيّ عمليّة من شأنها اخفاء المصدر غير المشروع الذي اكتسبت منه الأموال أصبح ميّسرا جدّا على الإنترنت إذ تخطّى الحواجز الحدوديّة بين الدّول و أصبح أكثر سريّة و خفاء.

ج) تجارة المخدّرات عبر الإنترنت:

انتشرت في السنوات الماضية مواقع على الإنترنت تشوّق الهواة و خاصّة المراهقين لاستخدام المخدّرات بل و تعلّمهم كيفيّة زراعتها و صناعتها بكافّة أصنافها و أنواعها و بأبسط الوسائل المتاحة. يقوم المراهق بالانزواء في غرفته والدخول الى تلك المواقع و من ثمّ تطبيق ما يقرأه بكلّ سريّة.

ح) الجرائم الجنسيّة وصناعة ونشر الإباحيّة:

رغم أنّ شبكة الإنترنت تعدّ من افضل الوسائل لنقل المعلومات المفيدة فانّها أيضا تعتبر من أخطر الوسائل لصناعة ونشر الإباحيّة. فهناك مواقع مخلّة بالحياء تحرّض على ممارسة الجنس للكبار و الصغار على حدّ سواء و ذلك بنشر الصور و الأفلام الإباحيّة التّي تستعمل في عروضها الأطفال و النّساء. هذا النّوع من الجرائم ينتشر خصوصا في الدّول الغربيّة و الآسيويّة.

خ) جرائم القذف و السبّ و تشويه السمعة:

تعتبر شبكة الإنترنت مسرحا غير محدود لأنها تلقى كل ما يدرج عليها دون رقابة. يقوم المجرم في الغالب بنشرمعلومات مغلوطة أو سريّة أو مضلّلة عن الضحيّة (مثال ما يعرض عبر موقع اليوتوب من أسرار المشاهير وعلاقاتهم).

د) جرائم انتحال الشخصيّة:

بمجرّد معرفة خصوصيّات الأفراد، تعتبر هذه الجرائم من أسهل الجرائم ارتكابا. يقوم المجرم بانتحال شخصية

اخرى بطريقة غير شرعية على الإنترنت بهدف الاستفادة من تلك الشخصية (الاستفادة من سمعتها أو مالها أو صلاحيّتها) أو لإخفاء هويّته لتسهيل ارتكابه لجرائم أخرى.

ذ) جرائم التغرير و الاستدراج:

التغرير والاستدراج وهما من أشهر جرائم الإنترنت وأكثرها انتشارا خاصة بين أوساط صغار السن من مستخدمي الشّبكة، وهذه الجريمة تقوم على عنصر الإبهام في تكوين العلاقات من قبل المجرمين الذين يوهمون ضحاياهم برغبتهم في تكوين صداقة على الإنترنت و التي قد تتطوّر الى التقاء مادّي بين الطرفين.

ر) الإرهاب:

يتمّ بثّ ثقافة الإرهاب عبر الإنترنت عن طريق تأسيس مواقع افتراضيّة تمثّل المنظمّات الإرهابيّة، وهي مواقع آخذة في الازدياد مع ازدياد المنظمّات الإرهابيّة، حيث تعلن عبر هذه المواقع تحملها مسؤوليّة احدى الهجمات التي ارتكبت، أوبيانات تنفي أو تعلق على أخبارصادرة عن منظمات أو جهات دوليّة أخرى. تجنّد الجماعات الإرهابيّة من خلال الإنترنت عناصر ارهابيّة جديدة تساعدهم على تنفيذ أعمالهم الإجراميّة ، وهم في ذلك يعتمدون على فئة الشّباب، خصوصا ضعاف العقل و الفكر[3].

ز) التجسّس:

لقد تقلّص دور الجواسيس الدوليين، الذي كان منتشراً أيام الحرب الباردة، واقتصر هذا الدّور على حالات خاصّة، وقلّت لذلك، الحاجة لتجنيد وتدريب أشخاص ذوي كفاءات ذهنيّة وبدنيّة عالية، لسنوات عديدة، ومن ثمّ دسهم في قلب نظام دولة معادية، لسرقة أسرارها، وتسريبها إلى دولتهم الأصليّة وتحوّلت طرق التّجسّس في عصر الإنترنت، إلى عمليّات تجسّس إلكترونيّة، واختراق لأنظمة وشبكات الدّول بعضها بعضاً. تستهدف عمليّة التجسّس في عصرنا الحالي ثلاثة أهداف رئيسيّة وهي: التجسّس السيّاسي، و التجسّس العسكري، و التجسّس الاقتصادي.

س) الجريمة المنظّمة:

تختلف الجريمة المنظّمة عن غيرها من الجرائم. فهي عبارة عن مجتمع اجرامي يعمل خارج اطار الشّعب و الحكومة وفق نظام بالغ الدّقّة و التعقيد. الجريمة المنظّمة ليست وليدة التقدّم التكنولوجي، بل هي استفادت منه. فأصبحت غير مقيّدة لا بزمان و لا بمكان. واستطاعت تمريروتنفيذ مخطّطاتها الإجراميّة عبر الإنترنت بكلّ سهولة و يسر.

تصنيف الجرائم المعلوماتيّة	
الدوافع	التنفيذ
• دوافع نفسيّة • دوافع جنسيّة • دوافع عقائديّة • دوافع عنصريّة	• فردي – فردي • فردي – جماعي • جماعي – فردي • جماعي – جماعي
الأهداف	الأنواع
• اثبات الذات • التّشفي و الانتقام • المتعة و التّسلية • الضّغط و الابتزاز	• التجّسس • الاتلاف و التّدمير • التّزوير • الخداع و التّغرير
الوسائل	
• البريد الالكتروني • الحاسب الآلي و برامجه • الهاتف المحمول و برامجه • شبكات المعلومات المحليّة و العالميّة (الإنترنت)	

شكل رقم (٤): تصنيف الجريمة المعلوماتيّة

٦. طرق الحدّ من الجرائم المعلوماتيّة

ازاء انتشار الجرائم الإلكترونيّة كظاهرة عالميّة، كان من الضّروري إيجاد حلول فعّالة واتّخاذ تدابير وقائيّة وردعيّة لوقف الزّحف الخطير للجرائم الإلكترونيّة التّي باتت تهدّد اقتصاديّات و أمن واستقرار الدّول، حيث قدّرت نسبة الشّكاوى الرّسميّة التّي اعتمدها المركز العالمي لشكاوى الانترنت عام ٢٠٠٠م باثني عشر بليون دولار جراء النّتائج

التّدميريـة التـي تـسبّبت فيهـا فيروسـات إتـلاف بـرامج المعلوماتيّة، وقدّرت نسبة الشّكاوى الرّسمية الّتي قدّمها الضّحايا للمركز بـ ٢٧٥٢٨٤ حالة . وكنتيجة لذلك، ومن أجل حماية فعّالة لبرامج المعلوماتية وقاعدة البيانات، يجب اعتماد كافّة السّبل القانونيّة الوقائيّة للحدّ من الجرائم الإلكترونيّة عن طريق كلمات مرور سريّة، مع الحرص على تغييرها دوريا، وتكثيف برامج الرّقابة على نوادي ومقاهي الإنترنت، وحجب المواقع الإباحيّة كما هو الحال بالمملكة العربية السّعودية وتونس، واعتماد برامج خاصّة مضادّة للفيروسات التدميريّة واستعمالها بشكل مستمرّ[5]. كذلك يتعيّن إدخال مادّة أخلاقيّات الانترنت ضمن المناهج الدراسيّة في التّعليم ما قبل الجامعي و نشر الوعي بين صفوف المواطنين خاصّة الشّباب بمخاطر التّعامل مع المواقع السيّئة على الانترنت و تعزيز التّعاون مع المؤسّسات الدّوليّة المعنيّة بمكافحة مثل هذه الجرائم وخلق قوانين خاصّة لمعالجة هذه الجرائم المستحدثة.

أ) التّعاون الدّولي للحدّ من الجرائم الإلكترونيّة:

يمكن تحقيق التّعاون الدولي للحد من الجرائم الإلكترونيّة عن طريق تبادل الخبرات في هذا المجال، وإيجاد نظام قانوني خاصّ لمواجهة هذا الخطر يبنى على أطر قانونيّة تراعي الطّبيعة المختلفة لجميع بلدان العالم، وتبنّي منظومة معلوماتيّة موحّدة تعتمد على إنشاء مكتب عالمي أو إقليمي للتّوثيق الإلكتروني، وتسجيل كافّة البرامج المعلوماتيّة وحفظها، واعتماد الدّلائل أو القرائن الرقميّة كدلائل إثبات الجريمة ومن ثمّة إدانة مقترفيها، والحرص على إدراج مثل هذه الجرائم ضمن اختصاصات المحكمة الجنائيّة الدوليّة نظرا لطابعها العالمي.

والجدير بالذّكر، أنّ المملكة العربيّة السّعوديّة كانت أوّل دولة عربيّة سنّت نظامًا خاصًا لمكافحة الجريمة الإلكترونيّة، تلتها الإمارات العربيّة المتّحدة، وبعد ذلك سلطنة عمان. غير أنّ الطبيعة الوطنيّة لهذه الأنظمة من جانب، والثّغرات القانونيّة الموجودة بها من جانب آخر، تجعلنا ندعو إلى سنّ نظام قانوني دولي يأخذ في اعتباره السّمة الافتراضيّة التي تتمّ فيها تلك الجرائم، يكون مبنيا على قاعدة معلومات موثّقة شاملة، وتدعيم أجهزة الأمن بما فيها الشّرطة الجنائيّة الدوليّة "الأنتربول" بكافّة المعطيات اللازمة لتكوين خبراء مختصّين في التقنية الإلكترونيّة [5].

ب) محاولات الحدّ من الجرائم الإلكترونيّة:

- أعلنت شركة "مايكروسوفت" في أواخر سنة ٢٠١٣ عن افتتاحها مركز الجرائم الإلكترونيّة في ولاية واشنطن بالولايات المتّحدة الأمريكيّة، وهو المركز الذي سيتخصّص في مراقبة نموّ الجرائم الإلكترونيّة ومكافحتها عالميّا. وأوضحت الشركة الأمريكيّة أنّ مركز "مايكروسوفت للجرائم الإلكترونيّة" (انظر الشّكل رقم (٥))، سوف يجمع بين الخبرة القانونية والتّقنية وكافّة الأدوات المتطوّرة لمكافحة تلك النوعيّة من الجريمة بشكل فعّال على شبكة الإنترنت. وأشارت "مايكروسوفت" إلى أنّ مركزها سيحاول المساهمة في الحدّ من كافّة أنواع الجريمة الإلكترونيّة سواء تلك المرتبطة بالبرمجيات الخبيثة أو سرقة الملكيّة الفكريّة أو حتّى تقنيات استغلال الأطفال. وسوف يحاول المركز التّصدي كذلك لشبكات "بوتنت" التّي بدأت في الإنتشار بشكل كبير مستغلّة حواسب الملايين من المستخدمين للقيام بجرائم إلكترونيّة دون علمهم، حيث قال ديفيد فين، المستشار العام المساعد في وحدة الجرائم الإلكترونيّة لدى الشّركة "الهدف الأوّل من هذا المكان هو جعل الإنترنت أكثر أمنا للجميع." أضافت "مايكروسوفت" أن المركز كذلك سيوفّر خبراته وقدراته للمساعدة في حل الجرائم الإلكترونيّة الكبيرة حول العالم، مثل جرائم الاحتيال عبر الإنترنت وسرقة الهويّة والتجسّس والاختراق. وأكّدت الشّركة الأمريكيّة أنّ الجرائم الإلكترونيّة تؤثّر سلباً على الاقتصاد العالمي حيث تبلغ تكلفة تلك الجرائم على الاقتصاد العالمي نحو ٥٠٠ مليار دولار أمريكي، خاصّة أن ٥٠ بالمائة من مستخدمي الإنترنت الرّاشدين وقعوا ضحيّة لجريمة إلكترونيّة في العام الماضي فقط. ومن جانبه قال نوبورو ناكاتاني، المدير التّنفيذي لمجمع الإنتربول (البوليس الدّولي) للابتكار، "المركز سوف يكون بمثابة محور هامّ في جهود التّصدي للهجمات الإلكترونيّة واستباقها[6]."



شكل رقم (٥): "مايكروسوفت للجرائم الإلكترونية"

في ظل تصاعد الخطر الإرهابي ، لاسيما من تنظيم داعش النّاشط على الأراضي العراقيّة والسوريّة، والذي رمى بشباكه مقتنصاً شباباً إسلامياً عربيّاً وأجنبيّاً، لاحظنا تسابقاً دوليّاً(قطر، ليبيا، المغرب، فرنسا،...) لسنّ قوانين وأنظمة تحول دون نموّالإرهاب على حساب أبنائها.

٧. الخاتمة

أردنا من خلال بحثنا هذا أن نضيء بعض جوانب الجريمة المعلوماتيّة قصد أخذ الحيطة والحذر، فهناك الكثير من الشركات والمؤسّسات والأشخاص لا يعيرون اهتماما جديّا لما يتعرّض له العالم اليوم من قرصنة وسرقة معلومات وجرائم عن طريق وسائل التكنولوجيا المتعددة. بل ساهم "الجهل الرّقمي" لمستعملي الإنترنت في ارتفاع معدل الجريمة الإلكترونيّة ممّا يستوجب وضع الحلول الجذريّة لمعالجة هذا النّوع من الجرائم أو الحدّ من تفشّيه داخل المجتمعات، و لا يمكن الشّروع في ذلك في ظلّ غياب مجلّة قانونيّة جامعة وشاملة لعقوبات زجريّة ضدّ المنفذين. وقبل تفعيل عمل الجهات الأمنيّة و القضائيّة للحدّ من هذه الظواهر المستجدّة التي تهدّد أمن الوطن و شعبه والعمل على مكافحتها بحكمة و حزم، وجب التأكيد على ضرورة تفعيل أساليب التوعية لدى مستخدمي الإنترنت وحثّهم على الاستخدام الأمثل لهذه التقنيات، و التّي من المفترض وجدت لخدمة الإنسان و ليس لمضرّته. أمّا بالنّسبة لمستخدمي الإنترنت من الشّعوب المسلمة، فالواجب لتوعيتهم احياء الوازع الديني عندهم. فالمانع من الوقوع في فتن وشرور الوسائل الإلكترونيّة وغيرها هو أن نقيم توحيد اللّه عزّ وجلّ خالصاً غضّاً طريّاً كما جاء في كتاب اللّه وسنّة رسوله صلّى اللّه عليه وسلّم، قال تعالى (ما يلفظ من قول إلا لديه رقيب عتيد) وقال أيضا (ولا تقف ما ليس لك به علم إنّ السّمع والبصر والفؤاد كلّ أولئك كان عنه مسئولا) و في الحديث الصّحيح قال رسول اللّه صلّى اللّه عليه وسلّم "من كان يؤمن باللّه واليوم الآخر فليقل خيرا أو ليصمت" وقال أيضاعليه الصّلاة و السّلام "المسلم من سلم المسلمون من لسانه ويده".

المراجع

[١] http://www.startimes.com/f.aspx?t=29897223

[٢] http://www.dhd4train.com/data/learn-with-us/crime/data/3.doc

[٣] الجريمة المرتكبة عبر الإنترنت.مذكرة لنيل شهادة الماجستير في القانون.تخصّص:القانون الدولي للأعمال.صغير يوسف، تيزي وزو،٢٠١٣.

[٤] المشكلات الأخلاقيّة و القانونيّة المثارة حول شبكة الإنترنت.مذكرة لنيل شهادة الماجستير في علم المكتبات.تخصّص:اعلام علمي و تقني.بلال بن جامع، قسنطينة،٢٠٠٧.

[٥] http://drabdsabor.blogspot.com/2014/08/blog-post_40.html

[٦] http://www.alarabiya.net/ar/technology/2013/